North Dakota Homeland Security Anti-Terrorism Summary

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

Quick Links

North Dakota

Oil tank explodes near Alexander. One man was injured when an oil tank exploded in McKenzie County, North Dakota on May 5, officials said. Four oil tanks owned by Landtech Enterprises were destroyed in the ensuing fire that lasted for hours, and smoke could be seen for miles. The blast occurred between 1:30 p.m. and 2 p.m., about 15 miles south of Williston, along U.S. Highway 85, near Alexander. The cause of the explosion is not yet known, said Landtech Enterprises' owner, who was at the scene Wednesday evening. He said one worker was hurt in the explosion, suffering burns, and was transported to Ramsey Burn Center in St. Paul, Minnesota. Source: http://www.willistonherald.com/articles/2010/05/06/news/doc4be2e06c1797b579427557.txt

Regional

(Minnesota) **Suspected Norovirus outbreak sickens 35 at church fundraiser.** The Minnesota Department of Health is continuing their investigation of a suspected Norovirus outbreak after 35 people reported ill following a church fundraiser April 25. In total, 275 people attended the event at Lakewood Evangelical Free Church in Baxter. The food was supplied by a caterer, Prairie Bay Restaurant, which is fully cooperating with the health department. The catered food was arranged in a buffet and staffed by volunteers who set up tables and cutlery. Officials are still unsure about the source of the virus. Because of the nature of a buffet-style event, Norovirus could have originated from a volunteer, a sick person in line who touched shared utensils or from the restaurant where the food was prepared. So far into the investigation, 60 people have been interviewed, 35 of whom reported symptoms of the virus. Officials expect to discover more victims as interviews continue. Source: http://eatdrinkandbe.org/article/index.0506_or_churchnoro

(Minnesota) **NRC schedules regulatory conference to discuss an issue related to Prairie Island Emergency Preparedness Program.** The Nuclear Regulatory Commission (NRC) staff will meet with the staff of Northern States Power Company, Minnesota, on May 11, to discuss a preliminary finding of low to moderate safety significance associated with the plant's emergency preparedness program. In May 2009 the utility informed the NRC about a problem with the plant's capability to declare an Alert emergency classification for certain events involving effluent releases from the plant. Specifically, the highest measurement capability of three effluent radiation monitors was too low to identify radiation levels that would lead the plant to declare an Alert, the second lowest of the NRC's four emergency classifications. In 2006, the plant adopted a new scheme for set points that would lead to different emergency declarations and the set point for declaring an Alert was increased. However, the utility failed to make changes to its program to ensure that Alerts would be declared in a timely fashion. There have been no actual emergency conditions at the plant that would have required an Alert declaration using this equipment. After the regulatory conference, the NRC will review the information received during the meeting and make a final determination on the safety significance of this issue. Source: http://www.nrc.gov/reading-rm/doc-collections/news/2010/10-015.iii.html

(Minnesota) **Columbia Heights man arrested after he threatened to destroy property at state capitol.** Authorities arrested a Columbia Heights, Minnesota man on Friday after receiving word he had made threatening statements about destroying property on the grounds of the Minnesota State Capitol building. Columbia Heights police working in conjunction with capitol security and the Bureau of Alcohol, Tobacco, Firearms and Explosives arrested the 57-year-old suspect in his home at 4 p.m., said a state patrol spokesman. The suspect was being held Friday night in the Hennepin County Jail in Minneapolis, pending charges. Authorities removed evidence from his home, which will be analyzed to determine if it posed an explosives threat, the spokesman said. Capitol security interviewed the suspect after learning of the threat through his acquaintances. They then consulted with the Hennepin County Attorney's office before pursuing the arrest. "He just made threats and some of them involved possible used of explosives," the spokesman said. Source: http://www.twincities.com/ci_14995199?nclick_check=1

National

(Washington) **Wind knocks out power; avalanche risk high in mountains.** An unusual winter-like storm swept through the Puget Sound area on May 3, knocking down power lines and increasing the risk of avalanches in the mountains. Wind gusts topped out at 47 mph in Everett by Monday afternoon. The high winds knocked tree branches onto power lines throughout Snohomish County. More than 15,000 people lost power throughout the day, a PUD spokesman said. Outages were reported in Marysville, Arlington, Smokey Point, Lake Stevens and Granite Falls, among other areas. By late evening, only 2,500 were without power. The National Weather Service has a winter storm warning in effect until 6 a.m. May 4 in the Cascades. The state Transportation Department has closed the North Cascades Highway because of avalanche danger. High winds and spring sunshine might make all that snow unstable, increasing the risk of avalanches, said the director of the Northwest Weather and Avalanche Center. The conditions can be particularly hazardous, since many people are not focused on avalanches in May, he said. Source: http://www.enterprisenewspapers.com/article/20100504/NEWS01/705049869/0/ETPZoneLT

International

Captured German tanker heads for Somalia: EU. A German-owned chemical tanker with an international crew of 22 appeared Sunday to be heading to Somalia, a day after its capture by pirates, a European naval task force said. The tanker "is heading back towards the Somali coast, it is clearly in the hands of pirates," a EU-NAVFOR spokesman told AFP, a day after armed pirates hijacked the 13,000-ton Marida Marguerite off Oman. The crew — made up of 19 Indians, two Bangladeshis, and a Ukrainian — were said on Saturday to be "well" by the anti-piracy task force, citing radio contact with the vessel. The capture added to at least 25 ships now held by ransom-seeking pirates, according to Ecoterra International, an environmentalist group monitoring maritime activity in the region. Source: http://www.google.com/hostednews/afp/article/ALeqM5gEd7JksLsYRTXefywx2klsuwmXcQ

Russian special forces storm oil tanker, free ship. Russian special forces rappelled onto a disabled oil tanker taken over by Somali pirates and freed 23 Russian sailors early Thursday, the commander of the EU Naval Force said. Ten pirates were arrested and one was killed. The raid on the Liberian-flagged ship Moscow University came 24 hours after pirates had taken the ship over and the crew

locked itself in a safe room. The vessel is carrying 86,000 tons of crude oil worth about $50 million. The special forces had been aboard the Russian anti-submarine destroyer Marshal Shaposhnikov, which rushed to the scene after Wednesday's seajacking. A helicopter was dispatched to investigate and was fired on by the pirates, EU Naval Force said. The Russian warship returned fire on the pirates, it said. Source: http://www.google.com/hostednews/ap/article/ALeqM5gB7YMEDuCwwY9ncDOtPAkEI4-H2wD9FH8U480

Ash grounds Irish, UK flights; summer chaos feared. Airspace over Scotland and Northern Ireland will be closed from early Wednesday because of volcanic ash that closed airports in Ireland on Tuesday and could threaten summer holiday travel. Britain's aviation authority said airports in northwest England and north Wales could also be affected by the ash from an Icelandic volcano which brought chaos to European air travel last month. Forecasts showed the concentration of ash in the atmosphere exceeded recommended safety levels, it said. "The situation is very dynamic, so passengers expecting to travel from the impacted airports should contact their airlines to check whether their flight is operating," the Civil Aviation Authority said on its website. Airspace over Scotland and Northern Ireland will be closed from 0600 GMT (7:00 a.m. British time) and airports in the two regions are also expected to close. Airports in Ireland and parts of Britain were closed for a number of hours on Tuesday. The latest disruption was caused by ash being blown from the same volcano in Iceland that caused mayhem for 10 million travellers last month. It was the first test of a European system of progressive closures, including partial no-fly zones, introduced after the abrasive ash cloud prompted a blanket ban that was criticised by airlines forced to ground thousands of flights in April. The IAA said northerly winds forecast for the coming days could bring more clouds of ash from the Icelandic eruption and disruption for passengers this week. "We could be faced with this periodically during the summer," the IAA Chief Executive said. "We are probably facing a summer of uncertainty due to this ash cloud." Source: http://uk.reuters.com/article/idUKTRE6431NA20100504

3 dead in fire at Greek bank during Athens riots. Three people died when an Athens bank went up in flames Wednesday as tens of thousands of Greeks took to the streets to protest harsh spending cuts aimed at saving the country from bankruptcy. Tear gas drifted across the city's center as hundreds of rioters hurled paving stones and Molotov cocktails at police, who responded with heavy use of tear gas. At least two buildings were on fire. The fire brigade said the bodies were found in the wreckage of a Marfin Bank branch, on the route of the march in the city center. An estimated 100,000 people took to the streets as part of nationwide strikes to protest austerity measures imposed as a condition of bailout loans from the International Monetary Fund and other eurozone governments. Source: http://www.google.com/hostednews/ap/article/ALeqM5iXUJvBknZVGqsBenIusBgBvWj5WQD9FGMT100

Accused Mariposa botnet operators sought jobs at Spanish security firm. The technical director and blogger for Spanish security firm Panda Security spent much of the last year helping Spanish police with an investigation that led to the arrest of three local men suspected of operating and renting access to a massive and global network of hacked computers. Then, roughly 60 days after the hackers' arrest, something strange happened: Two of them unexpectedly turned up at his office and asked to be hired as security researchers. He said he received a visit from them on the morning of March 22. The two men, known by the online nicknames "Netkairo" and "Ostiator," were arrested in February by Spanish police for their alleged role in running the "Mariposa" botnet, a malware

distribution platform that spread malicious software to more than 12 million Internet addresses from 190 countries. "Ostiator told me, 'The thing is, with everything that's been happening, we're not earning any money at the moment,' " the technical director recalled. "He said, 'We thought we could look for some kind of agreement in which both sides would benefit. We think we have knowledge [that] could be useful to Panda and thought we could have some kind of agreement with Panda.' " Netkairo and Ostiator have not yet been charged with any crime. The technical director asked them how they got started creating Mariposa. "Basically, they said they started it as kind of a hobby, and that they weren't working at the time," he said. "Suddenly, they started to earn money, a few hundred Euros a week to start, and then discovered they couldn't stop. And the whole time, their network kept growing." Source: http://krebsonsecurity.com/tag/luis-corrons/

Canada issues travel advisory over terror threat in Delhi. Canada is the latest country — after the U.S., the U.K. and Australia — in warning their citizens traveling to India about a threat of an imminent Islamist terrorist attack in New Delhi. This travel advisory was the third sent out in recent days, cautioning tourists to avoid New Delhi's popular Chandni Chowk area in Old Delhi. The U.S., the U.K. and Australia have also warned of imminent terror threat in New Delhi, particularly in market places like Connaught Place, Greater Kailash and Chandni Chowk, where crowds throng, especially during weekends. Reports citing intelligence sources said e-mails recently received from some servers in Pakistan by sports organizations in the U.K., Canada and Australia warn them not to send athletes to Delhi for the Commonwealth Games. Intelligence agencies also suspect that Islamic terrorists might be planning to target the infrastructure of the games, and participants and organizers ahead of the games. Meanwhile, it is reported that a Kashmiri Muslim was arrested for allegedly being a major part of a plan to attack Delhi this weekend. The Jammu and Kashmir police said the man, who was allegedly operating on behalf of the Pakistan-based Islamic terrorist group Lashkar-e-Toiba, confessed to his planned role to carry out bomb attacks in Delhi. He was to have picked up a consignment of explosives and reach Delhi April 27 to carry out the attacks, but was detained last week as part of a group of persons who threw stones at members of the security forces. Source: http://www.rttnews.com/Content/CanadianNews.aspx?Id=1289015&SM=1

Banking and Finance Industry

Financial crisis highlights need to improve oversight of leverage at financial institutions. In 2009, the U.S. Government Accountability Office (GAO) conducted a study on the role of leverage in the recent financial crisis and federal oversight of leverage, as mandated by the Emergency Economic Stabilization Act. This testimony presents the results of that study, and discusses (1) how leveraging and deleveraging by financial institutions may have contributed to the crisis; (2) how federal financial regulators limit the buildup of leverage; and (3) the limitations the crisis has revealed in regulatory approaches used to restrict leverage and regulatory proposals to address them. The crisis has revealed limitations in regulatory approaches used to restrict leverage. First, regulatory capital measures did not always fully capture certain risks, which resulted in some institutions not holding capital commensurate with their risks and facing capital shortfalls when the crisis began. Federal regulators have called for reforms, including through international efforts to revise the Basel II capital framework. The planned U.S. implementation of Basel II would increase reliance on risk models for determining capital needs for certain large institutions. The crisis underscored concerns about the use of such models for determining capital adequacy, but regulators have not assessed whether proposed Basel II reforms will address these concerns. Such an assessment is critical to ensure that

changes to the regulatory framework address the limitations the crisis had revealed. Second, regulators face challenges in counteracting cyclical leverage trends and are working on reform proposals. Finally, the crisis has revealed that with multiple regulators responsible for individual markets or institutions, none has clear responsibility to assess the potential effects of the buildup of system-wide leverage or the collective effect of institutions' deleveraging activities. Source: http://www.gao.gov/products/GAO-10-555T

Four banks fail May 7. State and federal regulators closed four banks Friday, May 7. These closings raise to 75 the number of failed institutions so far in 2010. The Bank of Bonifay, Bonifay, Florida, was closed by the Florida Office of Financial Regulation, which appointed the Federal Deposit Insurance Corporation (FDIC) as receiver. The First Federal Bank of Florida, Lake City, FL will assume all of the deposits of the failed bank. The failed bank had $242.9 million in total assets .The estimated cost to the Depositors Insurance Fund (DIF) will be $78.7 million. Access Bank, Champlin, MN, was closed by the Minnesota Department of Commerce, which appointed the FDIC as receiver. The bank's assets were sold to PrinsBank, Prinsburg, MN. Access Bank had $32 million in assets. The estimated cost to the DIF will be $5.5 million. Towne Bank of Arizona, Mesa, AZ, was closed by the Arizona Department of Financial Institutions, which appointed the FDIC as receiver. Commerce Bank of Arizona, Tucson, AZ will assume all of the deposits of the failed bank. The Towne Bank of Arizona branch will become a branch of Commerce Bank of Arizona. Towne Bank of Arizona had $120.2 million in total assets. The FDIC estimates that the cost to the DIF will be $41.8 million. 1st Pacific Bank of California, San Diego, California, was closed by the California Department of Financial Institutions, which appointed the FDIC as receiver. The six branches of 1st Pacific Bank of California will reopen as branches of City National Bank. 1st Pacific Bank of California had $335.8 million in assets. The estimated cost to the DIF will be $87.7 million. Source: http://www.bankinfosecurity.com/articles.php?art_id=2502

ATM users on alert after skimming cases along West Coast. An unidentified suspect is wanted by authorities in three different states, including Oregon. Police said he is stealing bank card numbers and pins using an ATM skimming device. He then produces cloned bank cards and pilfering accounts. A surveillance photo taken at a Vancouver, Washington, bank shows a white male, around 30 to 40 years old. Police said he has short brown hair, a mustache and a goatee. They said he's about 5'9" to 6 feet tall and has a stocky build. Vancouver is one area the suspect allegedly hit the hardest. Police said they are still looking for him. The case extends to California, Nevada, Idaho and Washington, with incidents occurring from August 2009 to April 2010. Source: http://kezi.com/news/local/173171

Input error leads to huge Dow Jones fall. The Dow Jones fell by nearly 1,000 points, and the Nasdaq and New York Stock Exchange announced that all trades more than 60 per cent above or below market that occurred between 2.40pm and 3.00pm New York time would be cancelled. The dramatic fall in the Dow Jones industrial average appears to have been caused by a trader hitting the button for 'billion' not 'million'. Proctor & Gamble shares fell by over a third on the day's trading. A report on CNBC said that the problem came when a deal involving Proctor & Gamble shares was incorrectly entered. "We, along with the rest of the financial industry, are investigating to find the source of today's market volatility," Citigroup said in a statement. "At this point we have no evidence that Citi was involved in any erroneous transaction." "We don't know what caused it," said a Procter & Gamble spokeswoman. "We know that that was an electronic trade, and we're looking into it with Nasdaq and the other major electronic exchanges." Source: http://www.v3.co.uk/v3/news/2262620/computer-input-error-leads

Fun with ATM skimmers, part III. According to the European ATM Security Team (EAST), a not-for-profit payment security organization, ATM crimes in Europe jumped 149 percent form 2007 to 2008, and most of that increase has been linked to a dramatic increase in ATM skimming attacks. During 2008, a total of 10,302 skimming incidents were reported in Europe. A short video authorities in Germany released recently showing two men caught on camera there installing a skimmer and a pinhole camera panel above to record PINs. EAST estimates that European ATM fraud losses in 2008 were nearly 500 million Euros, although roughly 80 percent of those losses resulted from fraud committed outside Europe by criminals using stolen card details. EAST believes this is because some 90 percent of European ATMs now are compliant with the so-called "chip and pin" or EMV (an initialism for Europay, Mastercard and VISA) standard. U.S. based financial institutions do not require chip-and-PIN, and that may be a contributor to the high fraud rates in the United States. The U.S. Secret Service estimates that annual losses from ATM fraud totaled about $1 billion in 2008, or about $350,000 each day. Source: http://krebsonsecurity.com/

How cyber-crooks turn stolen data into money on eBay. In a quickswapping scheme, a cyber-crook will use sites such as eBay or Amazon to offer an expensive item at a cheap price. After a deal is reached, the scammer will make an enticing offer — they will agree to ship the item to the buyer and only accept payment after the person has checked it out. Next, the scammer will use credit card information he or she previously pilfered with malware such as Zeus to purchase the item and send it to the buyer. After the buyer sends the agreed payment via Western Union or WebMoney, the scammer disappears, leaving the person whose card was stolen with an illegal charge and the quickswapping buyer at risk of having the item confiscated by police as stolen merchandise. While quickswapping is new, it is very similar to a reshipping scam. "As recently as two or three years ago, these types of scams were run by one to two individuals or groups, but as online fraud increases in both numbers and sophistication there has become a growing need for specialization within each portion of the scam," the senior manager of identity protection and verification at RSA told eWeek. Source: http://www.eweek.com/c/a/Security/How-CyberCrooks-Turn-Stolen-Data-into-Money-on-eBay-603320/

Hacker develops multi-platform rootkit for ATMs. One year after his Black Hat talk on Automated Teller Machine security vulnerabilities was yanked by his employer, a security researcher plans to deliver the talk and disclose a new ATM rootkit (bugs in the software used to run the machines) at the computer security conference. He will demonstrate several ways of attacking ATM machines, including remote, network-based attacks. He will also reveal a "multi-platform ATM rootkit," and will discuss things that the ATM industry can do to protect itself from such attacks. He was set to discuss ATM security problems at last year's conference, but his employer, Juniper Networks, made him pull the presentation after getting complaints from an ATM maker that was worried that the information he had discovered could be misused. Source: http://www.computerworld.com/s/article/9176371/Hacker_develops_multi_platform_rootkit_for_ATMs

Federal mortgage watchdog agency struggles with its information security. The Federal Housing Finance Agency has not fully implemented an information security program, resulting in weaknesses in its information technology security, according to the Government Accountability Office. GAO found that FHFA did not always maintain authorization records for network and system access, and did not

enforce least-privilege policies for system and application users. It also did not have adequate physical security and environmental safety controls for facilities housing IT resources. "Until the agency strengthens its logical access and physical access controls and fully implements an information security program that includes policies and procedures reflecting the current agency environment, increased risk exists that sensitive information and resources will not be sufficiently protected from inadvertent or deliberate misuse, improper disclosure, or destruction," GAO concluded. FHFA expects to have final access control procedures in place by June that will restrict access to administrators, application users, and others authorized by the information owners. "We are moving forward expeditiously to strengthen and complete implementation of FHFA's information security program," the acting director wrote in response to the GAO findings. Source: http://gcn.com/articles/2010/05/03/fhfa-security-050310.aspx

(California) **Community crime alert increase in credit card fraud.** In recent months, the City of Berkeley Police Department (BPD) in California has seen a spike in identity theft and credit card fraud. These cases may be in the City of Berkeley, but personal and credit card information is usually used by a larger national and international network of criminals. After community members' credit and bank accounts are compromised, suspects often use them at large retailers across the United States, with a high concentration in Texas, Louisiana, Michigan, and Georgia. BPD is investigating these cases and has some indications that they may be part of a larger data breach. Ultimately, BPD cannot confirm where the compromises originate. Source: http://www.ci.berkeley.ca.us/PressReleaseMain.aspx?id=53372

7 banks fail on April 30. State and federal banking regulators closed seven banks on April 30, including three banks in Puerto Rico — the first banks to fail in the U.S. commonwealth, as well as three of the largest institutions to close in 2010. Westernbank had $11.94 billion in assets; R-G Premier Bank, $5.92 billion; and Eurobank, $2.56 billion. These latest closings raise to 71 the number of failed banks and credit unions so far in 2010. The three Puerto Rican banks closed on April 30 included Eurobank, San Juan, Puerto Rico, R-G Premier Bank, and Westernbank. The three were closed by the Office of the Commissioner of Financial Institutions of the Commonwealth of Puerto Rico, which appointed the Federal Deposit Insurance Corporation (FDIC) as receiver for all three. The FDIC and Oriental Bank and Trust entered into a loss-share transaction on $1.58 billion of Eurobank's assets. The estimated cost to the Deposit Insurance Fund (DIF) will be $743.9 million. Source: http://www.bankinfosecurity.com/articles.php?art_id=2482

BBB warns that insurance scams are flourishing in current economy. In the midst of a tight economy and in the wake of the new national healthcare reform bill, State and Federal regulators are warning about a surge in healthcare-related scams. According to an October 2009 survey conducted by the Coalition Against Insurance Fraud, 57 percent of state fraud bureaus reported a higher incidence of health insurance fraud in 2009 compared to the previous year. The increase was largely attributed to "unauthorized entities selling fake coverage" and "the rise of medical discount plans." Companies such as HealthcareOne/Elite Healthcare, Consolidated Workers Association, and Smart Data Solutions/American Trade Association, have all recently come under fire from state regulators for peddling worthless coverage or discount medical plans — instead of actual insurance — to thousands of consumers. Additionally, shortly after the healthcare reform bill was signed into law, the U.S. Department of Health and Human Services issued a warning to consumers to beware of health insurance offers claiming to be part of new federal regulations. For example in Missouri, the State

Insurance director warned that a door-to-door salesman was claiming to be a federal agent selling insurance under the new law. Source: http://www.bbb.org/us/article/bbb-warns-that-insurance-scams-are-flourishing-in-current-economy-19245

Chemical and Hazardous Materials Sector

Agrichemical company allegedly imports misbranded pesticide. Albaugh, Inc., an agrichemical company based in Ankeny, Iowa, has agreed to pay a $27,360 civil penalty to the United States to settle allegations related to the importation of nearly 1,000 tons of misbranded pesticide from Argentina. According to a consent agreement and final order filed in Kansas City, Kansas, Albaugh violated the Federal Insecticide, Fungicide and Rodenticide Act (FIFRA) by importing a total of 1,990,440 pounds of the misbranded pesticide 2,4-D Acid to the Kansas City Port of Entry during March and April. The six shipments, comprising a total of 1,026 bags of the pesticide, were delivered to Albaugh's facility at 4900 Stockyards Expressway, in St. Joseph, Missouri. Under FIFRA, the bags were considered to be misbranded because they did not have required labeling that must include directions for the safe and proper use and handling of the pesticide. Albaugh was ordered to hold the material until it was relabeled with the correct information. As part of the consent agreement, Albaugh has certified that it is now in compliance with FIFRA and its regulations. Source: http://eponline.com/articles/2010/05/10/agrichemical-company-allegedly-imports-misbranded-pesticide.aspx

New US study on nuclear plant health risks hailed. Pennsylvania officials and activists say they are glad the federal government is taking another look at whether people who live near nuclear plants have a higher risk of getting cancer. The federal Nuclear Regulatory Commission announced last month that it was asking the National Academy of Sciences to do a "state-of-the-art study" on cancer risk for populations surrounding nuclear power facilities. The academy is being asked to update a 1990 study released by the National Cancer Institute that found no increased risk of cancer deaths in counties surrounding 62 nuclear facilities, "including all of the nuclear power reactors operational before 1982," the commission said. The NRC spokesman said the question of possible health effects comes up frequently from the public. "It's an appropriate time now," he said. "It's been two decades since this kind of national study." In addition, he said, the previous study looked only at data on the county level, and technology developed since then will allow for more refined breakdowns that could find clusters of health problems the previous study might have missed. The four- to five-year study will also look at all cancers rather than only at cancer deaths, he said. Source: http://www.businessweek.com/ap/financialnews/D9FFEAIG0.htm

US Labor Department's OSHA releases data detailing worker exposure to toxic chemicals. In keeping with the President's memorandum on open government, the U.S. Labor Department's Occupational Safety and Health Administration (OSHA) is releasing 15 years of data providing details of workplace exposure to toxic chemicals. The data is comprised of measurements taken by OSHA compliance officers during the course of inspections. It includes exposure levels to hazardous chemicals including asbestos, benzene, beryllium, cadmium, lead, nickel, silica, and others. The data offers insights into the levels of toxic chemicals commonly found in workplaces, as well as insights into how chemical exposure levels to specific chemicals are distributed across industries, geographical areas and time. "We believe this information, in the hands of informed, key stakeholders, will ultimately lead to a more robust and focused debate on what still needs to be done

to protect workers in all sectors, especially in the chemical industry," said the assistant secretary of Labor for OSHA. With an understanding of these data and their limitations, it can be combined with other related data to target further research into occupational hazards and illness. In addition to this raw data, OSHA will soon make available an easy-to-use online search tool allowing easy public access to this information. Source: http://www.dol.gov/opa/media/press/osha/osha20100583.htm

COMMERCIAL FACILITIES

(New York) **U.S. blames Pakistani Taliban for Times Square bomb plot.** The U.S. Attorney General said investigators had "developed evidence that shows the Pakistani Taliban was behind the attack," a sharp escalation from the initial assessment that the Time Square car-bomb suspect had acted alone and without sophisticated training. The Attorney General's remarks, coupled with similar statements by other senior U.S. officials over the weekend, highlighted the emerging role of an al-Qaeda-affiliated group that appears to have only recently moved to follow through on its ambition, expressed for years, of striking inside the United States. The suspect told investigators that he trained in Waziristan, a base of operations for al-Qaeda and the Pakistani Taliban in the mountainous border region near Afghanistan. The Times Square plot would mark the first time the Pakistani Taliban has tried to strike on American soil, signaling that the group may be moving beyond its earlier targets in Pakistan and, much more rarely, Afghanistan. A top counter-terrorism adviser at the White House said the administration is "taking very seriously" the threat posed by the Tehrik-e-Taliban, or TTP, calling it a "very determined enemy." Source: http://www.washingtonpost.com/wp-dyn/content/article/2010/05/09/AR2010050901143.html

(New York) **Official: NY car bomb suspect did a dry run.** Days before the failed car bomb in Times Square, a Pakistani-American scouted the bustling district in the same vehicle and then, on a second trip, left a getaway car blocks from his chosen target, a law enforcement official has told The Associated Press. The suspect drove a 1993 Nissan Pathfinder to Times Square from Connecticut on April 28, apparently to figure out where would be the best place to leave it later, the official said Wednesday. He then returned April 30 to drop off a black Isuzu, according to the official, who spoke on condition of anonymity because of the sensitive nature of the investigation. The Pakistani-American from Connecticut admitted to rigging the Pathfinder with a crude bomb based on explosives training he received in Pakistan, authorities say. He was pulled off a Dubai-bound plane Monday and has been cooperating with investigators. For a second day Wednesday, he had yet to appear in Manhattan federal court. Investigators had already started searching for suspects, when he returned to the scene on Sunday with a second set of keys to pick up the Isuzu, parked about eight blocks from the car bomb site, the official said. Source: http://www.signonsandiego.com/news/2010/may/06/official-ny-car-bomb-suspect-did-a-dry-run/

(California) **At least 4 stabbed in SoCal target, woman arrested.** A woman who stabbed and wounded four people in a busy Target store Monday afternoon was arrested when an off-duty sheriff's deputy pulled his gun and ordered the woman to the ground as screaming shoppers ran from the building, authorities said. The suspect started randomly stabbing people with a blade about the size of a kitchen knife at about 12:45 p.m. May 3, a Los Angeles sheriff's sergeant said. The 35-year-old was arrested with the help of private security guards. Several shoppers who saw the deputy pull out his weapon feared he was a gunman, adding to the sense of panic, the sheriff's sergeant said. "There's a bunch of screaming going on," he said. "He orders her to the ground. She complies." Three

women and a man were stabbed and taken to area hospitals, he said. The Los Angeles County Fire Inspector said one victim was in critical condition. Authorities did not immediately know the conditions of the others. The sheriff's sergeant said the deputy hero is a five-year veteran of the department and was authorized to have a weapon in the store. "Police officers can carry guns anywhere in the U.S.," he said. "I carry my gun everywhere. Most police officers carry a firearm all the time. We see a lot of bad guys at work." Source: http://www.foxnews.com/us/2010/05/03/stabbed-socal-target-woman-arrested/?test=latestnews

(Pennsylvania) **Suspicious device forces delay near marathon finish.** A suspicious device near the Pittsburgh Marathon finish line prompted police to stop the race for 10 to 12 minutes after the race leaders finished. The device was disabled, and the police said it was not believed to have been an explosive. A race spokeswoman said that the race was diverted around the block where the device was found but that the finish was not changed. Source: http://www.nytimes.com/2010/05/03/sports/03sportsbriefs-marathon.html

Communications Sector

AT&T dropping more calls than ever. AT&T announced in January that it was spending $2 billion this year to improve its much maligned cellular network. A survey of smartphone customers was released May 4 by ChangeWave Research, the consumer polling division of InvestorPlace.com. In a poll that asked 4,040 smartphone users in March how many dropped calls they had experienced in the past three months, AT&T — the exclusive U.S. carrier of Apple's iPhone and iPad mobile devices — came in last among the country's four largest carriers. Verizon customers reported losing only 1.5 percent of their calls over the past three months, the lowest in the smartphone industry and the lowest percentage for a carrier ever recorded by ChangeWave. AT&T customers, by contrast, reported 4.5 percent of calls dropped in the last three months. That is one out of every 22 calls — three times as many as Verizon's and the worst percentage ChangeWave has ever seen. Sprint was the country's second most reliable carrier, with 2.4 percent of calls dropped, and T-Mobile the third, with 2.8 percent of calls dropped. The survey was conducted between March 9 and March 23. Source: http://tech.fortune.cnn.com/2010/05/05/att-dropping-more-calls-than-ever/

FCC chooses a middle ground in enforcing net neutrality. The Federal Communications Commission has come up with a new way to apply some net neutrality rules that would force Comcast Corp., AT&T Inc. and other broadband Internet service providers to handle all Web traffic the same, without imposing limits on users or blocking websites. Its proposal released May 6 is aimed at blunting an April federal appeals court ruling involving Comcast that found the agency had limited authority to regulate broadband Internet service. FCC Chairman said in a statement that the Comcast decision had created a "serious problem" and that his agency believes more regulation of broadband Internet service is needed, though not the heavier restrictions that apply to telephone companies.The Democratic appointee to the commission said existing law allows the agency to apply a "narrowly tailored broadband framework" to regulate Internet traffic. His proposal seeks to give the agency direct authority over broadband service. Source: http://www.latimes.com/business/la-fi-internet-fcc-20100507,0,3891841.story

FCC chairman expected to leave broadband services deregulated. The chairman of the Federal Communications Commission (FCC) has indicated he wants to keep broadband services deregulated,

even as a federal court decision has exposed weaknesses in the agency's ability to be a strong watchdog over the companies that provide access to the Web. The FCC currently has "ancillary" authority over broadband providers such as Comcast, AT&T, and Verizon and must adequately justify actions against those providers. Last month, the U.S. Court of Appeals for the District of Columbia Circuit said the agency had exceeded its authority in 2008 when it applied sanctions against Comcast. The ruling cast doubt over the FCC's ability to create a "net neutrality" rule that would force Internet service providers to treat all services and applications on the web equally. The FCC Chairman is expected to respond soon to the court ruling. Three sources at the agency said that while the chairman has not made a final decision, he has indicated in recent discussions that he is leaning toward keeping in place the current regulatory framework for broadband services, while making small changes that would bolster the FCC's chances of overseeing some broadband policies. Source: http://www.washingtonpost.com/wp-dyn/content/article/2010/05/02/AR2010050203262.html?hpid=sec-tech

Defense Industrial Base Sector

Raytheon-Boeing team demonstrates JAGM can be employed from Super Hornet. Raytheon Company and The Boeing Company completed wind tunnel testing of the Joint Air-to-Ground Missile. The test proved the team's JAGM can be flown and employed from the F/A-18 E/F Super Hornet's outboard wing station. "The warfighter can place a full Raytheon-Boeing JAGM missile load on the outer wing stations, enabling the system to safely exceed the objective load-out requirement on the Super Hornet," said the Raytheon vice president of Advanced Missiles and Unmanned Systems. The Raytheon-Boeing offering features a Boeing body and warhead combined with a Raytheon tri-mode seeker. The tri-mode seeker, which leverages the same technology used on the Raytheon GBU-53/B Small Diameter Bomb II, enables the weapon to attack a variety of fixed and moving targets in all weather conditions. Source: http://nosint.blogspot.com/2010/05/raytheon-boeing-team-demonstrates-jagm.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+blogspot/fqzx+(Naval+Open+Source+INTelligence)

(Alabama) **2 dead after explosion at Ala. Army base.** Two contract workers died after being injured in an explosion while removing a propellant from rockets at Redstone Arsenal, where the Army conducts missile and weapons research. The public affairs office at the post in Huntsville said the two died Wednesday night after being flown to the burn unit at UAB Hospital in Birmingham. Both worked for a Redstone contractor, Amtech Corp., and were injured in an explosion at 8:45 a.m. Wednesday while removing ammonium perchlorate from rockets at a test site. There was no word on what caused the explosion, which left part of the building in wreckage. A third worker was nearby but escaped harm, and there was no environmental impact from the accident, the Army said. A statement from a Deputy Public Affairs Officer said the building recently passed safety inspections and was designed to minimize the impact of possible explosions, but "the work that we perform is inherently dangerous work." Source: http://www.google.com/hostednews/ap/article/ALeqM5ib9lO6WUJd3Owlp6BCvi2XcNBB3wD9FHE3RO0

Corps shows off long-delayed EFV. The Marine Corps celebrated the rollout of the first Expeditionary Fighting Vehicle on Tuesday, one day after the Secretary of Defense once again raised doubts about

the need for the multi-million dollar vehicle. Despite the renewed criticism, the hundreds of Marines and civilian contractors who showed up to the rollout ceremony at the National Museum of the Marine Corps had high hopes for the EFV, saying it is a "quantum leap forward in technology," and the start of a new chapter in the Corps' long and storied expeditionary history. The Corps, which hopes to purchase 573 vehicles, will test seven different prototypes. The prototypes will head to the amphibious vehicle test branch at Camp Pendleton, Calif., for additional testing. The Corps is expected to take possession of the first vehicle in June, and the remaining prototypes will be turned over to the Corps between July and October, officials said. The EFV has overcome numerous challenges. Widespread technical failures caused the Corps to scrap plans for the vehicle in 2007 and restart the program's entire development and demonstration phase, a move that cost nearly $1 billion and resulted in hundreds of design changes. The Corps will put the vehicle and those design changes through 500 hours of rigorous testing beginning this summer and ending in December, and Marine officials are anxiously standing by to see how it performs. Source: http://www.militarytimes.com/news/2010/05/marine_efv_rollout_050410/

Critical Manufacturing

Nissan recalls Infiniti G35 sedans, coupes. Nissan Motor Co recalled Infiniti G35 sedans and coupes affecting as many as 134,000 cars due to a connector that could cause airbags not to deploy during a crash, U.S. regulators said on Tuesday. The U.S. National Highway Traffic Safety Administration said as many as 134,215 Infiniti G35 sedans from model years 2005-2006 and G35 coupes from model years 2005-2007 are subject to the recall. The affected models were made at a Nissan plant in Japan. No injuries or accidents have been reported. NHTSA said a wire harness for the airbags may wear down to the point that it could interrupt a signal to deploy the airbags in the event of a crash. Most of the vehicles involved are in the United States, but cars are also recalled in South Korea, Canada, Puerto Rico, Taiwan, Guam, and the Middle East. Nissan informed federal officials of the potential problem two weeks ago, NHTSA reports show. Source: http://in.reuters.com/article/businessNews/idINIndia-48218420100504

GM recalls over 126,000 Hummer H3s. General Motors Co is recalling about 126,130 Hummer H3 models to address the risk that part of the hood could detach from the vehicle while driving. GM said in a filing with the National Highway Traffic Safety Administration that clips holding the hood louver on some of the vehicles could break, causing the part to break loose and strike a vehicle behind the Hummer in traffic. The recall covers 2006 through 2010 model year Hummer H3 vehicles. Source: http://www.reuters.com/article/idUSTRE6442M020100505?type=domesticNews

(Indiana) **U.S. probes potential Chrysler sticky pedal issue.** The National Highway Traffic Safety Administration said in a document posted on its website that five consumers reported that the accelerator pedal became stuck and would not return to the idle position when released. Elkhart, Indiana-based supplier CTS Corp made the pedals involved in the Chrysler investigation. CTS is also the supplier of pedals involved in Toyota Motor Corp's January recall of more than 2 million vehicles. Chrysler said its own review has found that consumer complaints were limited to about 10,000 Calibers built during a five-week window in March and April 2006. The NHTSA probe covers some 161,000 Dodge Calibers built for the 2007 model year. Chrysler and NHTSA said they were not aware of any accidents, injuries or property damage related to the issue. "It appears to be a supplier manufacturing concern, which is mechanical in nature and not a design or electronic issue," Chrysler

said in a statement. The automaker also said the vehicle is equipped with a brake override system, which allows the engine controller to reduce power and stop the car when both the brake and the accelerator are depressed. CTS representatives were not immediately available to comment. Source: http://www.reuters.com/article/idUSTRE6422KO20100503?feedType=RSS&feedName=domesticNews

Emergency Services

(Illinois) **Bensenville police get 'suspicious package'.** Bensenville, Illinois, police were investigating a "suspicious package" received at the main police station Sunday afternoon. A dispatcher said the package arrived at the station at 100 N. Church Road about 2:15 p.m., but she did not have details on how it arrived. There was no evacuation from the building, she said. Police and fire officials are inspecting the package. No further information was available. Source: http://www.chicagobreakingnews.com/2010/05/bensenville-police-get-suspicious-package.html

(Kentucky) **Thieves targeting fire stations.** Kentucky firefighters believe they are the target of a group of thieves, after break-ins at two different fire stations this week. The first break-in occurred at a fire station in Lewis County. Then there was another one just a few miles down the road at a station in Rowan County, discovered Saturday. That one was caught on tape. The surveillance video from the Route 377 fire station shows what appears to be three men casing the station about two o'clock Friday morning. The men broke into a storage building, but didn't steal anything. The fire chief believes an alarm system scared them off before they hit the station's main building. Source: http://www.lex18.com/news/thieves-targeting-fire-stations

DHS wants fire service to join fusion centers. The Department of Homeland Security Secretary said America's firefighters are truly the face of homeland security. Addressing about 1,800 at the annual CFSI Fire and Emergency Services dinner Thursday night, she announced a move to officially make the fire service an official partner in fusion centers, a clearinghouse for terrorist information. Fusion centers — recommended following the federal investigation of the Sept. 11 terrorist attacks — are staffed by federal employees. She encouraged responders to keep their eyes and ears open for suspicious activity. "The integration of fire service organizations and personnel into the fusion process enhances the efforts of all homeland security partners across all mission areas," officials said in a document entitled Fire Service Integration for Fusion Centers. The Secretary said it only makes sense that the people who are intimately familiar with their communities be included in the intelligence gathering. Source: http://www.firehouse.com/news/top-headlines/dhs-wants-fire-service-join-fusion-centers

Energy

(Georgia) **Southwire missing $500,000 in copper.** A brazen heist last month has Southwire and law enforcement officials wondering what happened to $500,000 worth of copper. The theft reportedly occurred on April 29, but was reported to Carrollton, Georgia police on May 4. Three 18-wheeler trucks — green, white, and red in color — arrived that day and were loaded with copper destined for Indiana. The trucks displayed the name of L. Transport in arch style writing. The trucks had been sent to Southwire by an independent broker for the purpose of making the Indiana delivery. The broker

had received faxed information for these loads showing the trucking company name to be LaRolle Transport out of Miami/Hialeah, Florida. "LaRolle states these are not their trucks," a Carollton Police police lieutenant said. "The broker received paper work for LaRolle but the trucks themselves had L. Transport on them." The loads did not arrive as scheduled in Indiana, and the identity of the true owners of the trucks is unknown. The Southwire spokesman said the drivers appeared to have all the proper documents to pick up the shipment, but the documents were indeed fakes. He described the theft as an "isolated incident." The Georgia Bureau of Investigation is now involved and Carrollton Police have made contact with law enforcement officials in Hialeah, Florida, who are also assisting with the case. Source: http://www.times-georgian.com/view/full_story/7343540/article-Southwire-missing--500-000-in-copper?instance=TG_home_story_offset

(Louisiana) **Safety fluid was removed before oil rig exploded in Gulf.** The investigation into what went wrong when the Deepwater Horizon exploded April 20 and started spilling millions of gallons of oil into the Gulf of Mexico is sure to find several engineering failures, from cement seals that did not hold back a powerful gas bubble to a 450-ton, 40-foot-tall blowout preventer, a stack of metal valves and pistons that each failed to close off the well. There was, however, a simpler protection against the disaster: mud. An attorney representing a witness says oil giant BP and the owner of the drilling platform, Switzerland-based Transocean Ltd., started to remove a mud barrier before a final cement plug was installed, a move industry experts say weakens control of the well in an emergency. A lawyer for a rig worker who survived the explosions said the mud was being extracted from the riser before the top cement cap was in place, and a statement by cementing contractor Halliburton confirmed the top cap was not installed. Mud could have averted catastrophe. If all of the mud had still been present, it would have helped push back against the gas burping up toward the rig, though it might not have held it back indefinitely. Source: http://www.nola.com/news/gulf-oil-spill/index.ssf/2010/05/safety_fluid_was_removed_befor.html

(Louisiana) **Cost of oil spill could exceed $14 billion.** Since an explosion almost two weeks ago on the Deepwater Horizon rig, a disaster scenario has emerged with hundreds of thousands of gallons of crude oil spewing unchecked into the Gulf and moving inexorably northward to the coast. The responsibility for the cleanup operation lies with the owners of the well, led by 65 percent shareholder, London-based oil company BP Plc. BP said last week that it was spending $6 million a day on the clean up but admitted this figure would rise sharply when the slick hits land. Neither the company or its 25 percent partner, explorer Anadarko Petroleum, have put an estimate on total costs, although BP's CEO told Reuters in an interview on Friday that he would pay all legitimate claims for damages. Source: http://www.reuters.com/article/idUSTRE6412H820100502

Food and Agriculture

New report shows gaps in FDA's food import oversight. The Food and Drug Administration (FDA) needs more authority to oversee imported foods, the Government Accountability Office (GAO) has said in a new report. There are about 189,000 registered foreign sites where food is made for sale in the United States, according to the report. Of those, the FDA inspected just 153 in 2008. Last year, it estimated that it would inspect 200 sites, and 600 in 2010. Meanwhile, the amount of food imported into the United States is increasing, and now accounts for 15 percent of the total food supply, including 60 percent of fresh fruits and vegetables and 80 percent of seafood. "GAO identified certain statutory authorities that could help FDA in its oversight of food safety," the report said. "Specifically,

GAO previously reported that FDA currently lacks mandatory recall authority for companies that do not voluntarily recall food products identified as unsafe. Limitations in FDA's food recall authorities heighten the risk that unsafe food will remain in the food supply." The findings of the GAO report were presented at a House committee hearing May 6, along with the findings of a previous study released in September last year in which the GAO said the FDA and USDA should work together to close gaps in the food safety network. The new GAO report is at www.gao.gov/new.items/d10699t.pdf. Source: http://www.foodproductiondaily.com/Supply-Chain/New-report-shows-gaps-in-FDA-s-food-import-oversight

(Massachusetts) **Imported manouri cheese voluntarily recalled due to potential Listeria contamination.** Mt. Vikos, Inc., a Marshfield, Massachusetts, firm is voluntarily recalling all size packages and all lot numbers of Mt. Vikos Brand Manouri - Sheep & Goat's Milk Cheese because it has the potential to be contaminated with Listeria monocytogenes, an organism which can cause serious and sometimes fatal infections in young children, frail or elderly people, and others with weakened immune systems. Distributed nationwide, the cheese has the Mt. Vikos Manouri label and comes in clear plastic packaging in 4-oz. portions for the retail market, and in 1-kilogram logs for the food service market. The company is asking food-service customers to notify consumers who may have purchased the product. The company has notified their customers and has pulled the product. No illnesses have been reported to date in connection with this problem. Source: http://www.fda.gov/Safety/Recalls/ucm211207.htm

E. coli outbreak sickens 19 people in three states. A food company has recalled lettuce sold in 23 states and the District of Columbia because of an E. coli outbreak that has sickened at least 19 people, three of them with life-threatening symptoms. The Food and Drug Administration (FDA) said May 6 that 12 people had been hospitalized and the federal Centers for Disease Control and Prevention (CDC) said it was looking at 10 other cases probably linked to the outbreak. Freshway Foods of Sidney, Ohio, said it was recalling romaine lettuce sold under the Freshway and Imperial Sysco brands because of a possible link to the E. coli outbreak. College students at the University of Michigan in Ann Arbor, Ohio State in Columbus and Daemen College in Amherst, New York, are among those affected, according to local health departments in those states. The FDA is focusing its investigation on lettuce grown in Arizona as a possible source for the outbreak, according to two people who have been briefed by the agency. Freshway Foods said the lettuce was sold to wholesalers, food service outlets, in-store salad bars and delis. The company issued a statement May 6 that said the FDA informed it about the positive test in New York, May 5. The statement said "an extensive FDA investigation" of Freshway Foods' facility in Sidney has not uncovered any contamination at the plant. The recalled lettuce has a "best if used by" date of May 12 or earlier. The recall also affects "grab and go" salads sold at Kroger, Giant Eagle, Ingles Markets, and Marsh grocery stores. The lettuce was sold in Alabama, Connecticut, the District of Columbia, Florida, Georgia, Illinois, Indiana, Kansas, Kentucky, Maryland, Massachusetts, Michigan, Missouri, New Jersey, New York, North Carolina, Ohio, Pennsylvania, Rhode Island, South Carolina, Tennessee, Virginia, West Virginia, and Wisconsin. Source: http://www.foxnews.com/story/0,2933,592365,00.html?test=latestnews

(Kentucky) **Ky. agriculture hard hit by flooding.** Flash flooding that swamped stretches of cropland has left some farmers facing the costly prospect of starting over with spring planting as Kentuckians continued to assess damage from the deadly torrents of weekend rain. More than half of Kentucky's

counties declared states of emergency, and the governor May 5 asked the U.S. Department of Agriculture (USDA) for federal disaster assistance for drenched Kentucky farmers. Across rural Kentucky, it's too early to put a dollar figure on crop losses, but in some areas more than half the corn crop was probably destroyed in portions of western Kentucky, said a spokesman for the state Department of Agriculture. The wheat crop suffered significant damage, he said, but the situation "may be salvageable" for many farmers, depending on the depth of flood waters and how soon they recede. There were reports of widespread damage to fences, barns and other farm buildings, he said. In a letter to the USDA Secretary May 5, Kentucky's governor noted that the flooding had impacted all facets of Kentucky's agricultural industry even though the flooding has not yet reached its peak. The governor's office said the written request was the first step toward the process of obtaining a Secretarial Disaster Declaration, which would make federal assistance available to farmers statewide. Source: http://www.kentucky.com/2010/05/05/1253381/ky-agriculture-hard-hit-by-flooding.html

(Wisconsin) **Salmonella bacteria again detected in Nestle morsels.** For the second time this year, Nestle's Burlington, Wisconsin plant has shut down a production line after a positive salmonella test. Workers reported, and the company confirmed, that a batch of chocolate chips tested positive for salmonella April 28. A Nestle spokeswoman said the batch was made April 22, and the results came back several days later. That production line was shut down for "thorough additional cleaning," the spokeswoman said April 30. She said cleaning would continue through the weekend, and that production was expected to resume May 3. The spokeswoman said none of the contaminated morsels left the plant. A single sample of chocolate chips tested positive for salmonella, she said. Nestle tested batches before and after that one, and they all tested negative. Although only one production line was affected, Nestle will test for salmonella throughout the plant, and investigate to determine the source. She said raw agricultural products, such as cocoa beans, can carry salmonella. In mid-February, Nestle's acknowledged a similar incident where it discovered salmonella during routine testing. Then, as now, none of the contaminated product ever left the plant; it was later destroyed. That investigation proved inconclusive as the cause, the spokeswoman said. Source: http://www.journaltimes.com/news/local/article_48831052-549c-11df-805a-001cc4c002e0.html

(Hawaii) **New pest could destroy Hawaii's honey industry.** A beetle that's plaguing the United States mainland and has the potential to destroy bee hives is now on the Big Island of Hawaii. The state agriculture department said it could have a huge impact on Hawaii's multi-million dollar honey and queen bee export business. The threat is from the small hive beetle, which despite its small size — about a quarter of an inch — can cause big problems The beetle feeds on honey, pollen, wax, and honey bee eggs. The larvae can tunnel through the honeycomb which contaminates the honey and can lead to the death of hives. This also can affect the production of queen bees. "How it got here we have no idea. But part of the problem is that it not only survives in bee hives, but also on fruit so if there's rotting fruit on the ground like mangoes or guava, the beetles will breed in that as well," said a state agriculture department employee. A beekeeper on a Pana'ewa farm discovered the beetles in his hives last week, and then contacted the state agriculture department. The U.S. Department of Agriculture confirmed that the bugs were small hive beetles. Staff at the department of agriculture staff began surveying parts of the Big Island today, looking at bee hives and fruit. Source: http://www.khon2.com/news/local/story/New-pest-could-destroy-Hawaiis-honey-industry/Z7bdepLiSUujYCQm2jgvmA.cspx

(Illinois; Indiana) **Illinois firm recalls imported prosciutto products due to potential listeria contamination.** Orlando Greco & Son Imports, a Carol Stream, Ill., firm, is recalling approximately 822 pounds of prosciutto products that may be contaminated with Listeria monocytogenes, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced today. Specifically, the FSIS is recalling various pound cases of "Prosciutto Boneless Casa Italia" products. The problem was discovered by FSIS testing of imported product. FSIS was notified by the Canadian Food Inspection Agency that the implicated product was also distributed to an importer of record and further distributed. FSIS has received no reports of illness. The products were distributed to restaurants and retailers in Illinois and Indiana. Source: http://www.fsis.usda.gov/News_&_Events/Recall_028_2010_Release/index.asp

Gulf seafood in commerce safe to eat. As 200,000 gallons of crude oil continue to flow unabated into the Gulf of Mexico, government officials, seafood industry groups, and food safety experts are working to assure the public that seafood coming from the Gulf is safe for consumption. On May 2, the National Oceanic and Atmospheric Administration (NOAA) closed a 6,800 square mile section of the Gulf to recreational and commercial fishing to keep potentially unsafe, petroleum-contaminated seafood out of the food supply, but there is palpable concern in the fishing industry that consumers will think harvested seafood from the region is unsafe. "We will definitely not want to be anywhere near any type of oil spill to harvest any shrimp, if they were even in that area," one experienced shrimper based in Chalmette, Louisiana told Food Safety News. "The Louisiana Coastline is expansive, more than 300 miles long, and provides Louisiana fishermen an abundance of clean water areas in which to fish," the Louisiana Restaurant Association said in a statement this week. "According to the Louisiana Department of Wildlife and Fisheries' biologists, 77 percent of our seafood production comes from the west side of the Mississippi River, which is not in the impacted area." According to the head of environmental and occupational health sciences at the Louisiana State University School of Public Health, "[I]f the seafood smells like gasoline, if it smells like petroleum, then consider it tainted and don't eat it. If on the other hand it looks fresh, smells fresh, it tastes fresh, it's probably okay. The seafood, we know depending on the species, has a great capacity either to avoid contamination or ultimately to cleanse itself." Source: http://www.foodsafetynews.com/2010/05/gulf-seafood-in-commerce-is-safe-to-eat/

R-CALF: South Korean FMD outbreak source should alarm Homeland Security. R-CALF USA sent formal correspondence May 4 to the U.S. Department of Homeland Security Secretary to urge her to reverse the decision to relocate veterinary research on highly contagious diseases from Plum Island, New York, to the heart of cattle country – Manhattan, Kansas. The International Society for Infectious Diseases (ISID) has reported that a new outbreak of the foot-and-mouth disease (FMD) virus was confirmed in South Korea in a state-run livestock and veterinary science institute in South Chungcheong Province, South Korea. Prior to this latest outbreak, ISID reported that South Korea had experienced 16 outbreaks since January 1, 2010. Of particular interest is that ISID also reported that: "Quarantine control and decontamination efforts carried out at the site (the state-run livestock and veterinary science institute) are much more stringent than normal farms, raising concerns that the nationwide effort to contain the disease may not be effective." So far, according to ISID, more than 49,000 Korean animals were ordered to be culled as a result of that country's ongoing outbreaks. "Based on South Korea's ongoing FMD experience, combined with the clear evidence USDA lacks the ability to predict not only the actual risk of FMD, but also, the capacity to measure the effectiveness of measures designed to control FMD outbreaks, we are concerned any action by the U.S.

Department of Homeland Security to allow live FMD viruses on the U.S. mainland will result in the potential for FMD release and subsequent infection in U.S. livestock," the letter concludes. Source: http://www.cattlenetwork.com/R-CALF--South-Korean-FMD-Outbreak-Source-Should-Alarm-Homeland-Security/2010-05-04/Article_Latest_News.aspx?oid=1065014&fid=CN-LATEST_NEWS_

(Colorado) **Colorado firm recalls pork-sausage products for possible Listeria contamination.** Custom Corned Beef, Inc. of Denver is recalling approximately 460 pounds of fully cooked, crumbled pork-sausage products that may be contaminated with Listeria monocytogenes, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced May 1. The recall covers 10-pound boxes, with two, 5-pound packages of Polidori, Fully Cooked Pork Sausage Crumbles, Keep Refrigerated/Frozen. Each box label bears the establishment number "EST. 4121" inside the USDA mark of inspection. The fully cooked crumbled pork sausage products were produced on Apr. 9, 2010, and were distributed to institutional establishments in Colorado. The problem was discovered by a receiving federal establishment who had recently been tested by FSIS for Listeria monocytogenes. There have been no reports of illnesses yet associated with consumption of this product. Source: http://www.fsis.usda.gov/News_&_Events/Recall_027_2010_Release/index.asp

(New York; New Jersey) **Firm recalls Havista brand white fungus.** Northern Food I/E Inc. of Hicksville, New York, is recalling its 100-gram packages of Havista brand "white fungus" because they contain undeclared sulfites. People who have a sensitivity to sulfites run the risk of serious or life-threatening reactions if they consume this product. The product comes in a 100-gram clear plastic bag with a multi-color label on the front and a white label on the back. The product is coded Best Before 09/10/2011. The fungus was distributed in New York and New Jersey in retail stores. The recall was initiated after the sulfites were uncovered through routine sampling by the New York State Department of Agriculture and Markets Food Inspectors. The consumption of 10 milligrams of sulfites per serving has elicited severe reactions, including anaphylactic shock in some asthmatics. Analysis of the Havista fungus revealed it contained 124 milligrams per serving. No illnesses have been reported to date. Source: http://eatdrinkandbe.org/article/index.0503_or_whitefungus

Government Sector (including Schools and Universities)

(New York) **2 NY teens arrested in plot to attack high school.** A 17-year-old with a grudge against his former Long Island, New York high school planned with his girlfriend to buy shotguns, enter his old school and indiscriminately shoot down students and teachers, days before his ex-classmates were scheduled to graduate, police said May 7. The two teenagers extensively researched bomb making, attempted to buy a shotgun and set a June 10 date for the planned attack on Connetquot High School in Bohemia, a Suffolk County police sergeant said. Evidence from the 16-year-old girl's computer and cell phone showed they had searched bomb-making and explosives Web sites, and exchanged text messages in which they discussed plans to buy firearms and kill people, police said. Both were arrested and charged as adults with conspiracy. The boy pleaded not guilty at his arraignment May 7, while his girlfriend entered a not-guilty plea last week. Each could face up to a year in jail if convicted. Source: http://www.google.com/hostednews/ap/article/ALeqM5hMAjanxTBPm4bq3Ph_FSNHKxpnsgD9FID3600

Cloud security: Feds on cusp of change. The federal government is on the cusp of fundamental changes in the way it manages information-technology security risks, but those risks will grow more complicated as agencies begin embracing on-demand computing, according to a panel of public-sector, cloud-computing experts. The discussion was part of a May 4 technology conference on cloud computing, knowledge management and open-government innovations. Sponsored by 1105 Government Information Group, the convention took place in Washington, D.C. Coincidentally, the Treasury Department confirmed on the same day that it had shut down four Web sites hosted by a cloud-service provider after a security analyst found malicious code. Security in a cloud computing environment needs to be considered as three distinct areas, said the director of Cisco's Cloud and Virtualization Solutions. Security risks — and rules duplicating the work agencies must go through to certify the security of their information systems — remain one of the biggest obstacles to adopting cloud-computing strategies, said a computer scientist at the National Institute of Standards and Technologies and vice chair of the federal government's Interagency Cloud Computing Advisory Council. He outlined how a new government program called FedRAMP aims to address that problem by streamlining the certification process, so that an information-technology application certified for one agency will be available for all agencies to use. This would help industry too, he said. Source: http://fcw.com/Articles/2010/05/05/Securing-risks-in-the-cloud---Fed-on-the-cusp-of-change.aspx?p=1

(New Hampshire) **Cops say NH student tosses 'bomb bag' into school.** New Hampshire police said an 18-year-old high school student is facing charges that he threw what is being described as a "bomb bag" into a classroom. Manchester police said the suspect threw a bag into the classroom at the city's West High School, which made noise and began to expand before erupting in a minor explosion. The students in the classroom backed away for safety. Police described the device as a novelty item containing sodium bicarbonate and citric acid that was designed for outside use only. Police said that just before the incident, the school resource officer had just escorted the suspect off school property. Police said he was found with an additional "bomb bag." The suspect was charged with criminal trespass and disorderly conduct. Source: http://wbztv.com/wireapnewsnh/NH.student.charged.2.1678908.html

(Indiana) **Bomb threats empty four schools in Gary.** Police and school district officials are working to identify who called in a string of bomb threats at four Gary, Indiana Community School Corp. schools Wednesday morning. Initial calls were made at around 7:30 a.m. to West Side and Roosevelt high schools, Lincoln Achievement Center and Banneker Achievement Center, both elementary schools. Police believe all four calls originated from the same person, but declined to provide additional information while they investigate leads in the case. No one was injured and investigators found no evidence of bombs at any of the school buildings. The cost for emergency response services will be passed onto the individual who made the calls, according to a spokeswoman for Gary public schools. "Our priority is to keep students safe," the spokeswoman said, "and to identify the person and hold them responsible." Students were evacuated and waited in fields or playgrounds nearby the schools until the superintendent's office received word that the campuses were secure. Police determined the calls were placed by a voice that sounded like a young man's, the spokeswoman said. Earlier calls into the high schools and Lincoln made threat demands asking for $1 million to be dropped at various road intersections. Source: http://www.post-trib.com/news/lake/2240834,new-gthreats0506.article

(California) **Bomb threat closes College of the Sequoias temporarily.** A bomb threat forced the evacuation of thousands of College of the Sequoias (COS) students just after 11 a.m. May 4. The Visalia, California college's human resources office received a non-specific threat via telephone, a COS spokesman said. The voice was male, he said. An order was given to clear out every building and move staff and students to the parking lots on the perimeter. "I was waiting to go into my English class and the teacher told us we had to leave the building right away," a student said. "Usually this is a drill situation, but this time you could tell that it was serious." Police cordoned off the area and brought in fire and ambulance units. Teams from the Visalia Police Department and the college spent two hours combing though buildings with the help of a bomb-sniffing canine on loan from the Farmersville Police Department. COS campus police took the lead in the search and investigation, a Visalia police spokesman said. Nothing suspicious was found and the all clear signal was given at 12:45 p.m. Source: http://www.visaliatimesdelta.com/article/20100505/NEWS01/5050313/Bomb+threat+closes+College+of+the+Sequoias+temporarily

(Wisconsin) **Bomb squad called to investigate suspicious package near Army recruiting center.** The bomb squad was called to a Brookfield, Wisconsin, shopping center to examine a suspicious package outside the Armed Forces Recruiting Center. The squad determined the package was not dangerous. Recruiters at the center called police to report the package after they saw someone acting suspiciously. Businesses nearby were evacuated as a precaution. Police are trying to figure out who left the boxes and why. Source: http://www.fox6now.com/news/witi-100506-suspicious-package,0,3787386.story

(Washington) **Coweeman student found with homemade explosive.** Kelso, Washington police arrested a Coweeman Middle School student May 4 on suspicion of possession of explosives and a dangerous weapon on school grounds. The student was found in possession of a homemade explosive, which contained a very small amount of black powder, according to a police report. The student also had an illegal knife. The student was arrested without incident. There was no indication he intended to harm any students, police said. Source: http://www.tdn.com/news/local/article_cc4ec92a-57e0-11df-a121-001cc4c03286.html

(Indiana) **Gelatin prompts evacuation of Census Bureau office.** The discovery of red powdered gelatin in an envelope containing a completed census form prompted a five-hour evacuation of the U.S. Census Bureau's national processing center in Jeffersonville, Indiana on May 4. A worker opening envelopes containing returned census forms spotted the powder in an envelope about 8 a.m., said the director of the Census Bureau National Processing Center. When employees could not identify the powder, supervisors evacuated about 200 workers and called 911, bringing in police, firefighters and the Indiana National Guard's hazardous materials team. Workers returned to the building, which is across the Ohio River from Louisville, Kentucky, about 1 p.m. Tuesday, after the hazardous materials team identified the substance as powdered gelatin. "Our protocol is to evacuate the building, so we had roughly 200 people who had been outside for quite awhile," the director said. "We wanted to make sure it was safe for them to go in, and we'd get them back in out of the sun." Source: http://www.wsbt.com/news/regional/92777114.html

(Arizona) **Police analyzing white powder from letter mailed to Arizona Capitol.** State police are testing a white powdery substance and investigating a letter sent to the Arizona Capitol. The capitol

police chief said a staffer who works for the Arizona governor opened a letter Tuesday morning that contained a suspicious white substance. The Executive Tower at the Capitol complex in Phoenix was locked down for about 30 minutes. The building was later reopened, and the capitol police chief said state police are analyzing the substance to see if it is dangerous. Details about the letter were not disclosed. Source: http://phoenix.bizjournals.com/phoenix/stories/2010/05/03/daily25.html

(Florida) **Student arrested in Arnold High bomb hoax.** Authorities arrested an Arnold High School senior Monday afternoon, after a suspicious device was found in the Florida school's bathroom. The 18 year-old suspect was charged with manufacturing a hoax explosive device, a second-degree felony, and taken to the Bay County Jail after telling investigators he made the device with the "purpose of gaining popularity by pulling off a memorable senior prank and getting everyone out of class," according to a Bay County Sheriff's Office news release. "This kind of thing is so dangerous on so many levels," the Bay District schools superintendent said. "It was scary to students, parents and faculty members. â_¦ We have seen senior pranks before, butâ_¦ this was planned and premeditated." Officials said a student reported finding the suspicious device taped to the bottom of a sink in the boy's bathroom in the cafeteria about 7:15 a.m. The student reported it to the school's resource deputy, and students were ushered into the stadium as they arrived. School and law enforcement officials described the device as a cell phone that had parts of wires and a Game Boy sticking out, but it contained no chemical or explosive material. Source: http://www.newsherald.com/news/road-83530-alf-students.html

Treasury: Cloud computing host hacked. The Treasury Department blamed a cloud computing provider for the disruption of its Web site that provides the Internet face of the Bureau of Engraving and Printing, the agency that prints U.S. currency. A blog Monday reported that the sites were hacked. As of Tuesday afternoon, the bureau's Web site was inaccessible. On Tuesday, Treasury issued the following statement: "The Bureau of Engraving and Printing (BEP) entered the cloud computing arena last year. The hosting company used by BEP had an intrusion and as a result of that intrusion, numerous websites (BEP and non-BEP) were affected. On May 3, the Treasury Government Security Operations Center was made aware of the problem and subsequently notified BEP. BEP has four Internet address URLs all pointing to one public website. Those URLs are; BEP.gov; BEP.treas.gov; Moneyfactory.gov and Moneyfactory.com. BEP has since suspended the Web site. Through discussions with the provider, BEP is aware of the remediation steps required to restore the site and is currently working toward resolution." Treasury did not identify the host company. The chief research officer for IT security software vendor AVG wrote in his blog that "for a short while (Monday) a couple of treas.gov websites were hacked, and were reaching out to an attack site in Ukraine." He added: "They had been script injected with the line of code. BTW, you should not mess with the attack site. It was dead earlier (Monday), but could easily come back to life." Source: http://www.bankinfosecurity.com/articles.php?art_id=2488

(South Carolina) **Students face charges after bomb prank.** Two St. James High School students face possible expulsion and charges due to a prank involving a suspicious package found at the school April 29, according to a Horry County police report. Authorities were called to the school around 3:15 p.m. after school officials called 911 about a suspicious package. The package was isolated by the Horry County fire department and was in police custody for testing. The St. James High principal told police that four students had walked into the front office and stated that they had found a note that read "Bomb. I have laced this letter has anthrax, have a nice day and you will die a slow and painful

death." The note was signed by another student, whose parents were contacted by police. The four victims were checked out by the Horry County Fire Rescue's Hazmat team and released to their parents. The case will go before a magistrate who will decide whether to issue an arrest warrant. Source: http://www.thesunnews.com/2010/05/01/1451191/police-students-face-charges-after.html

Obama takes direct aim at anti-government rhetoric. In a blunt caution to political friend and foe, the U.S. President said Saturday that partisan rants and name-calling under the guise of legitimate discourse pose a serious danger to America's democracy, and may incite "extreme elements" to violence. The comments, in a graduation speech at the University of Michigan's huge football stadium, were the President's most direct take about the angry politics that have engulfed his young presidency after long clashes over health care, taxes and the role of government. "What troubles me is when I hear people say that all of government is inherently bad," the President said. "When our government is spoken of as some menacing, threatening foreign entity, it ignores the fact that in our democracy, government is us." Source: http://www.google.com/hostednews/ap/article/ALeqM5juui7didNwh_vzBmJyrbjxkeF-IgD9FE6UV00

(Utah) **Teachers train to prepare for terror attacks.** One local elementary school is getting prepared in case of a terror attack. Teachers at Sunset Elementary School in Davis County, Utah, went through training Friday afternoon, so they would know what to do to keep their students safe. Safety experts were on hand to educate the teachers about weapons and how they work, in case they encounter them in the classroom one day. Teachers also learned self-defense, the safest way to barricade their classroom, and what to expect if a SWAT team enters the school. The principal of Sunset Elementary said he wants his teachers prepared for any situation that may put students in danger. Source: http://www.abc4.com/content/news/slc/story/Teachers-train-to-prepare-for-terror-attacks/ld0AvBacE0CS1k1O7pIu5Q.cspx

Information Technology and Telecommunications

New attack bypasses virtually all AV protection. Researchers say they have devised a way to bypass protections built in to dozens of the most popular desktop anti-virus products, including those offered by McAfee, Trend Micro, AVG, and BitDefender. The method, developed by software security researchers at matousec.com, works by exploiting the driver hooks the anti-virus programs bury deep inside the Windows operating system. In essence, it works by sending them a sample of benign code that passes their security checks and then, before it's executed, swaps it out with a malicious payload. The exploit has to be timed just right so the benign code is not switched too soon or too late. But for systems running on multicore processors, matousec's "argument-switch" attack is fairly reliable because one thread is often unable to keep track of other simultaneously running threads. As a result, the vast majority of malware protection offered for Windows PCs can be tricked into allowing malicious code that under normal conditions would be blocked. All that is required is that the AV software use SSDT, or System Service Descriptor Table, hooks to modify parts of the OS kernel. Source: http://www.theregister.co.uk/2010/05/07/argument_switch_av_bypass/

Worms attack Skype, Yahoo Messenger. Security researchers have reported a new wave of attacks targeting users of Yahoo Messenger and Skype. BKIS (Bach Khoa Internetwork Security) researchers May 7, said the attack comes via messages such as, "Does my new hairstyle look good? bad? perfect?" and "My printer is about to be thrown through a window if this pic won't come our right.

You see anything wrong with it?" The messages contain malicious links. "The users are more easily tricked into clicking the link by these messages, because users tend to think that 'their friend(s)' are asking for [advice]," said the BKIS blog post. "Moreover, the URL shows a .jpg file to users, reinforcing the users' thought of an image file." BKIS' discovery follows the appearance of another worm targeting Yahoo Messenger that was reported recently. "The page at the end of the link is basic and does not employ any exploits in order to install the worm, it relies solely on social engineering to trick victims into believing they are opening a picture from a friend, while in fact they run the worm," explained a Symantec researcher May 2. Once executed, "the worm copies itself to %WinDir%\infocard.exe, then it adds itself to the Windows Firewall List, blocks the Windows Updates service and sets the following registry value so that it runs whenever the system boots: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"Firewall Administrating" = "%WinDir%\infocard.exe," the researcher wrote. With that done, the worm then blasts itself out to everyone on the victim's Yahoo Messenger contact list, and it may also download and execute other malicious files. Source: http://www.eweek.com/c/a/Security/Security-Researchers-Report-Attacks-on-Skype-Yahoo-Messenger-199929/

Dodgy Facebook pages used to power 'spam a friend' joke scam. Dubious Facebook pages host rogue Javascript code that creates a means for miscreants to spam people on a user's friends list, security researchers warn. A security researcher at Sunbelt Software, who goes by the online name Paperghost, explains that the ruse relies on duping prospective marks into completing surveys. Users who complete these studies would inadvertently grant access to their friends list by following instructions on misleading dialogue boxes. Baits being used in the ruse offer supposed access to the "world's funniest joke," among other ruses. Users are taken through a series of steps that results in them copying and then pasting JavaScript code into their address bar. Once this happens a "suggest this to your friends" dialogue box will automatically appear briefly on users' screens before it is replaced by a captcha prompt. Users who follow through will post a spam-link on the news feed of anybody who happens to be their friend. This "spamvertised" link, in turn, promotes a fake Internet survey aimed at flogging "expensive ringtones, and fake iPod offers, as explained in a blog post. A depressing total of over 600,000 links to four pages containing the malicious JavaScript reveals that numerous users have been exposed, if not already taken in, by the scam. Source: http://www.theregister.co.uk/2010/05/10/facebook_spam_friend_scam/

Breaches rise in U.K. firms along with wireless, VoIP, social networking. According to recent survey by Pricewaterhouse Coopers, more than 90 percent of large organizations (more than 250 employees) say they suffered a data breach in the past year, up from 72 percent in 2008, the last time the survey was conducted. About 83 percent of small organizations (50 or fewer employees) were hit last year, up from 45 percent in 2008. On average, large U.K. firms were hit with 45 breaches in the past year, three times as many incidents as they reported in 2008. Small firms were hit with an average of 14 breaches, more than two times the number they logged two years ago. At the same time, U.K. organizations are rapidly adopting new technologies and services. Nearly half use voice-over-IP (VoIP) — up from 17 percent two years ago — and 85 percent run wireless networks, twice as many as in '08. Social networking is important to business for 32 percent of the organizations, and 34 percent say they are "critically dependent" on cloud-based, hosted software services. Meanwhile, staffers lost or leaked confidential data in 46 percent of the large organizations, with 45 percent of those saying the information exposed was "very serious" or "extremely serious." Source:

http://www.darkreading.com/database_security/security/attacks/showArticle.jhtml?articleID=224701015

Facebook bug allowed users to eavesdrop on chats. Facebook engineers on Wednesday disabled the site's live chat function after people outside the company discovered a bug that allowed users to eavesdrop on their friends' conversations. The site also had to take emergency action to correct a separate hole that allowed users to see their friends' pending friend requests. Ironically, the gaffes were the result of a new "preview my profile" service Facebook added late last month in an effort to give users more control over their privacy settings. In a statement issued a few hours after the bug was reported by TechCrunch, Facebook said it temporarily suspended the chat function while it patched the information leak. With that work completed, it said it expected to turn chat back on "shortly." Over the past month, Facebook has been under siege by a variety of critics who say the site is imperiling the privacy of its 400 million or so users. Source: http://www.theregister.co.uk/2010/05/05/facebook_eavesdropping_bug/

Security risks of web application programming languages. A new WhiteHat report examined the security of specific programming languages. Nearly 1,700 business-critical websites were evaluated to provide organizations with insight into the relative security of the development frameworks they deploy, and the associated vulnerabilities that put them at risk. Perl had the highest average number of historical vulnerabilities found at 45 percent followed by Cold Fusion at 34 percent. Additionally, Perl, Cold Fusion, JSP and PHP were most likely to contain at least one serious vulnerability at approximately 80 percent of the time. Among the lowest historical vulnerability averages were ASPX (Microsoft's .NET) and DO (Struts Java) with 19 percent and 20 percent, respectively. WhiteHat's latest report contains data collected between January 1, 2006 and March 25, 2010, and finds that the percentage of high, critical or urgent issues continue to slowly increase. Vulnerability remediation rates are climbing as well, particularly in the Urgent and Critical categories, with an average rate of roughly 70 percent. Still, with up to 30 percent of vulnerabilities remaining open for an average of nearly three months, many websites remain in an uncomfortable risk position. Cross-Site Scripting (XSS) maintains its position in the Top 10 list along with many other common classes of attack. Cross-Site Request Forgery (CSRF) did not make the Top 10 list for languages such as Perl and PHP, but Directory Indexing did. The diversity of vulnerability issues across languages can be attributed to the fact that one website can possess hundreds of unique issues from a specific class such as XSS and Content Spoofing, while other sites may not contain any. Source: http://www.net-security.org/secworld.php?id=9252

Fast-spreading P2P worm targets USB drives. A crafty new P2P worm appears to be spreading quickly among users of a range of popular file-sharing programs. The worm lures victims using a link embedded in a spam IM message, which leads to what appears to be an image file but is actually the malicious payload. From that point on, the malware burrows into the host by installing a number of files that compromise the Windows XP firewall. By this point the criminals have control over the system and can open backdoors to install further malware or capture passwords entered using Internet Explorer or Mozilla Firefox. Two elements make Palevo.DP, the worm, interesting. First, it copies itself to network shares from the infected PC as well as USB sticks or other external drives. Any unprotected system with the Windows autorun feature turned on — basically almost every PC — will find itself infected as those drives are moved from PC to PC. The second feature is its targeting of P2P services by adding code to shared program files. The combination of removable media and P2P gives

the worm a two-pronged attack-and-spread strategy which allows it to target home systems which are then used to launch attacks on better-defended business PCs from inside the network perimeter. Source: http://www.networkworld.com/news/2010/050510-fast-spreading-p2p-worm-targets-usb.html?hpg1=bn

Wi-Fi key-cracking kits sold in China mean free Internet. Dodgy salesmen in China are making money from long-known weaknesses in a Wi-Fi encryption standard, by selling network key-cracking kits for the average user. Wi-Fi USB adapters bundled with a Linux operating system, key-breaking software, and a detailed instruction book are being sold online and at China's bustling electronics bazaars. The kits, pitched as a way for users to surf the Web for free, have drawn enough buyers and attention that one Chinese auction site, Taobao.com, had to ban their sale last year. With one of the "network-scrounging cards," or "ceng wang ka" in Chinese, a user with little technical knowledge can easily steal passwords to get online via Wi-Fi networks owned by other people. The kits are also cheap. A merchant in a Beijing bazaar sold one for 165 yuan (US$24), a price that included setup help from a man at the other end of the sprawling, multistory building. To crack a WEP key, they capture data being transmitted over the wireless network and target it with a brute-force attack to guess the key. The brute-force attacks on WPA encryption are less effective. But while WEP is outdated, many people still use it, especially on home routers, said one security researcher in China. That means an apartment building is bound to have WEP networks for a user to attack. "No matter where you go, you can use the Internet for free," the researcher said. Source: http://www.computerworld.com/s/article/9176318/Wi_Fi_key_cracking_kits_sold_in_China_mean_free_Internet

New IM worm spreading fast. A smiley-faced Instant Message (IM) with a photo link posing as if it is from someone on a user's buddy list is actually spreading a worm on Yahoo Instant Messenger: The IM ultimately delivers a worm that allows an attacker to take over the victim's machine, and to spread the worm to people on the victim's contact list. Researchers at BitDefender, BKIS, and Symantec May 3, each separately warned Yahoo Messenger users about the worm attack, which is rapidly growing. A researcher for BitDefender says his team has seen infection rates as high as 500 percent per hour in his home country of Romania since they first spotted it last week. He expects the worm to make inroads in the United States May 3 and May 4, with potential victims coming off of a weekend. The worm — known as Palevo by BitDefender, W32.Ymfocard.fam.Botnet by BKIS, and W32.Yimfoca by Symantec — is a new variant of an existing worm. In the Yahoo IM attack, it tricks the user into saving what appears to be a JPG or GIF file, but instead is a malicious executable. BitDefender said the worm contains a backdoor to install more malware, steal files, intercept passwords, and launch spam or other malware attacks on other systems. According to Symantec, once the worm is run, it adds itself to the Windows Firewall list, stops the Windows Update service, and configures itself such that it runs each time the system boots. The worm automatically sends itself to everyone on the victim's contact list. Source: http://www.darkreading.com/insiderthreat/security/attacks/showArticle.jhtml?articleID=224700541

Microsoft fixes bug in Producer software. Microsoft has released a new version of its Producer software, fixing a critical security problem that plagued the product for several months. Last March, Microsoft warned of a critical security bug in the product, but it did not release a new update. Instead, it said that Producer 2003 users should simply uninstall their software. On Monday, however, Microsoft posted an update, and is now recommending that "all customers using Producer 2003

upgrade to the new version," according to a blog post from the Microsoft Security Response Center. The flaw, which has to do with the way Producer reads certain file formats, also affects Windows Movie Maker. But Microsoft issued a Movie Maker patch when it first warned of the issue in March. A similar product, Windows Live Movie Maker — which runs on Vista and Windows 7 — is not affected by the issue. Microsoft does not know of anyone exploiting the bug in online attacks, but it is worried that hackers might be able to use it to install unauthorized software on victims' computers. Source: http://www.computerworld.com/s/article/9176280/Microsoft_fixes_bug_in_Producer_software

Infosec 2010: Large firms overwhelmed by security breaches. A staggering 92 percent of large organizations have suffered a security incident or data breach in the past year, as they struggle to cope with the changing threat landscape, according to the latest biennial Information Security Breaches Survey from PricewaterhouseCoopers (PwC). PwC branded the findings, released April 28 at Infosec 2010, as "surprisingly bad," and said that companies are struggling to mitigate the increased external threat levels and the large numbers of accidental breaches from insiders. "We were not expecting the results to be as significant as that. Right now it looks quite serious in terms of the costs," said a spokesman. "People are maintaining expenditure on security, but serious threats are rising and people are having to adapt and change to the new threat landscape." The report found that the median number of data breaches rose from five, two years ago to 45 today, and that the average costs had risen roughly threefold. Breaches totaled around Â£10bn in costs, with a big increase in the cost of reputation damage. Source: http://www.v3.co.uk/v3/news/2262177/infosec-2010-large-firms

Google 'personal' search bug exposed user Web history. Google has restored its "personalized" search suggestions after purging the tool of a critical vulnerability that allowed attackers to steal a user's Web history. Personalized search suggestions were disabled on March 1after a trio of security researchers — one at the University of California, Irvine and two at the French National Institute for Research in Computer Science and Control (INRIA) — sent Google a preliminary version of a paper showing how they were able to infer large portions of a user's Web history by hijacking the user's session ID (SID) cookie and nabbing the company's personalized-suggestion data. Then, on March 15, the company sent a statement to the researchers saying it had added SSL decryption to Google Web History and that it had started encrypting the back-end Web History server requests used to personalize suggestions on its Maps site. Google also said it would "soon" do the same for search, and this happened more than a month later. Google tells The Register that personalized search suggestions took longer to restore because the fix was "more complex to deploy and involved a larger code change." In a statement Google said, "We highly value our relationship with the security-research community, and we are grateful to the researchers from INRIA and University of California, Irvine who have been in contact with us since the end of February about their findings related to open, unsecured network connections and personalized suggestion technology." Source: http://www.theregister.co.uk/2010/04/29/google_personalized_suggestions_turned_off_after_researcher_attack/

National Monuments and Icons

(Montana) **Yellowstone developing Old Faithful area plan.** Yellowstone National Park has begun to develop a long-range plan for the Old Faithful area. The public can submit comments until June 7. Officials said they need a plan to identify ways to enhance visitors' experiences and accommodate

park operational needs while protecting resources in the area. In accordance with the National Environmental Policy Act, Yellowstone National Park will prepare an environmental assessment for the Old Faithful area during the next 16 months. Officials said the environmental document will provide a deeper understanding of resources through inventories, focus on resource protection and address visitor connections to the resources. The process will also evaluate alternative proposals and their potential impacts to multiple resources, including natural, cultural and scenic, as well as visitor use and experience, park operations and public health and safety. Source: http://www.jhnewsandguide.com/article.php?art_id=5956

(Colorado; Wyoming) **Beetle-killed areas may see closures, forester says.** A top U.S. Forest Service (USFS) official said he might have to close off national forests in Wyoming and Colorado unless more work is done to cut down beetle-killed trees near roads, trails and campsites. The USFS regional forester told U.S. Congressmen, May 4 that he expects 100,000 trees a day to fall in the forests of Colorado and southern Wyoming over the next decade. Trees are falling on roads and trails and are a safety concern, the forester told the U.S. House Agriculture Committee, which discussed the beetle epidemic during a field hearing in Cheyenne, Wyoming. "We've had several near misses already," he said. The forester said that more than $100 million would be needed to finish the tree-clearing work on the more than 3,000 miles of forest roads. But Wyoming's governor was skeptical about the need to close forests — a touchy proposition in a state where people love to hunt, hike, camp and fish and frequently second-guess the motives of federal-land managers. "I think that is a bit of an overreaction," the governor said in a news conference later. Beetles have been killing pine forests across the West over the past decade. Late last year, the USFS allocated $40 million to clear some of the 3.6 million acres of beetle-killed forest in Colorado and Wyoming. Source: http://billingsgazette.com/news/state-and-regional/wyoming/article_e6a2f580-57fe-11df-b60f-001cc4c002e0.html

(Kentucky) **Flooding closes roads and ferries in Mammoth Cave National Park.** Mammoth Cave National Park in Kentucky was affected by flooding as a result of 10 inches of rain that fell May 1-2. Currently, both Green River Ferry and Houchin Ferry are closed. The river has risen 35 feet and was not expected to crest until May 5. Once the river level drops, park staff will assess damage and remove mud and debris from the ferry landings. Every effort will be made to have both ferries back in service as soon as possible. Several park roads have been closed temporarily as a result of flooding impacts. Green River Ferry Road is closed on the south side of the park, and on the north side below the Maple Springs Campground. Houchin Ferry Road is closed on the south side, and on the north side beyond the Temple Hill Trailhead. The Ugly Creek/Little Jordan Road is closed. Dennison Ferry Day Use Area is closed. Cave tours continue to operate on regular schedules. Temporary adjustments have been made to the routing of the Historic Tour and the Violet City Lantern Tour as a result of flooding impacts. These tours will resume their usual routes as soon as conditions in the cave have returned to normal. Park staff are currently evaluating storm and flood impacts on the park's frontcountry and backcountry trails. While no trails have been closed at this time, visitors are advised to exercise caution in areas where trails may be blocked or eroded. All other park resources and facilities remain open. Source: http://www.nps.gov/maca/parknews/floodingimpacts_5-3-2010.htm

(Florida) **South Florida prepares for arrival of oil slick.** Powerful water currents could drag oil slick that resulted from a drilling explosion in the Gulf of Mexico to the southern Florida coast, threatening national parks. Outer bands of the powerful Loop Current moved north to within 31 miles of the

destroyed wellhead, that is spewing thousands of barrels a day. If the current reaches the spill, it could drag the slick south to the Florida Keys within days, and push it north to Broward and Palm Beach counties in a week to two weeks, marine scientists said May 3. "If it continues to move in that direction, and there is no reason why it shouldn't, the Loop Current could very well be at the wellhead," said a marine scientist, who is using satellite images to track the slick at the College of Marine Science at the University of South Florida. "So there is a strong likelihood that at some point in the future oil will be entrained into the Loop Current." On May 3, Florida's governor extended a state of emergency south to Sarasota County. Everglades National Park, Big Cypress National Preserve, Dry Tortugas National Park and Biscayne National Park began disaster preparations, establishing a response team comparable to that set up for hurricanes, and May 4 they will begin assessing vulnerable natural systems, such as mangrove shorelines. Source: http://articles.sun-sentinel.com/2010-05-03/news/fl-loop-current-20100503_1_beaches-slick-oil

Postal and Shipping

(Texas) **Building at SAC evacuated after suspicious package found.** A suspicious envelope forced the evacuation of a building at San Antonio College near downtown just before 11:00 a.m. May 6. The Fletcher Administration Center was evacuated and police, firefighters, and members of the Hazardous Materials Response Team were called in to investigate. Although the envelope was unopened, a skin rash developed on a mail room employee who handled the package. EMS was observed applying bandages to the employee's arms at the scene. San Antonio College officials said the hazmat team determined the material was not airborne and not explosive, but were unsure what caused the skin reaction. Everyone was allowed to return to the building around 12:30 p.m. The letter was removed from the building, decontaminated, and will be analyzed further. The envelope is addressed to the SAC International Studies Department, and originated from overseas, possibly from the Country of Qatar. Source: http://www.woai.com/mostpopular/story/Building-at-SAC-evacuated-after-suspicious/XQzZrUljdkOLje2W0erZkw.cspx

(Texas) **Device in FedEx box was meant to burn, not to explode, Colleyville police say.** A device in a FedEx box that a woman opened at her home Sunday was incendiary, intended to burn rather than explode, the Colleyville Police Chief said Monday. The cardboard box contained other objects, the police chief said, but he declined to describe them, citing the ongoing investigation by police and the federal Bureau of Alcohol, Tobacco, Firearms and Explosives. At a news conference, the police chief played part of the 911 call the woman made about 11 a.m. Sunday from her home in the 1000 block of Dogwood Court. "I opened it and there was a battery in it," she told the 911 operator. "My neighbor said it looks like a home-made bomb." She told police that she didn't hear a delivery truck and that no one had knocked on her door. "We still don't know how long that box had been there," said a police spokesman. "It's still too early in the investigation to say whether the homeowner was the target or not." The Northeast Explosive Response Team used a remote-controlled vehicle and water cannon to render the device safe, and components have been sent to an ATF office in San Francisco to try to determine who made it, the police chief said. No one was injured. But when asked whether the woman who opened the box had been lucky, the police chief said, "Absolutely." Source: http://www.star-telegram.com/2010/05/03/2161010/device-in-fedex-box-was-meant.html

Transient accused of anthrax hoax. A transient from Roseville and San Francisco accused of mailing anthrax hoax letters to federal offices has been indicted on 10 counts. He faces four counts of hoax

mailings, four counts of mailing threatening communications, one count of threatening the president, and one count of crossing state lines after failing to register as a sex offender. He is accused of sending envelopes to Social Security Administration offices in New York, Kansas City, and Baltimore on January 30. The U.S. attorney's office said the envelopes had a white powder inside and a card reading "you stole my money" and "die." According to the U.S. attorney's office, the White House got a similar envelope with a newspaper picture of the U.S. President that had crosshairs drawn over his face. He was arrested April 22 in San Francisco. Source: http://www.kcra.com/news/23312182/detail.html

(Illinois) **FBI investigating powder scare at Deere.** The Federal Bureau of Investigation is now the lead agency investigating a hazardous materials scare Friday at the John Deere Seeding Group in Moline, Illinois. Firefighters and a hazardous materials, or HAZMAT, team were dispatched to the plant at 501 River Drive at 3:46 p.m. after a suspicious substance was found on the outside of an envelope, said the Moline deputy fire chief. The envelope containing an unknown white powder was discovered in the facility's mailroom, said a Deere & Co. spokesman. Authorities temporarily shut down River Drive and kept about 100 employees inside the facility, officials said. The HAZMAT team concluded the substance was not hazardous in nature, he added. The envelope is at the State Laboratory in Springfield for testing, the deputy fire chief said. Manufacturing was not interrupted, the spokesman said. The workers at the site are responsible for maintenance and other similar duties, he said, adding that they were sent home for the night. Manufacturing operations were not scheduled at the plant over the weekend. Source: http://qctimes.com/news/local/crime-and-courts/article_a5e42356-558e-11df-8b51-001cc4c03286.html

PUBLIC HEALTH

Cancer risks prompt doctors to try to lower imaging scan radiation. Doctors are exploring ways to reduce the amount of radiation exposure from medical imaging tests in light of renewed concerns about the cancer risk, according to research presented at a radiology conference this week. Medical radiation from exams such as CTs, or computed tomography, causes 29,000 new cancers a year, a report in the Archives of Internal Medicine showed in December. An accompanying article found that the scans may expose people to four times as much radiation as previously estimated. The Food and Drug Administration is considering safeguards for CT scanners and other imaging machines. Radiologists have been working for several years to reduce unnecessary radiation exposure in children, whose growing bodies are more sensitive to radiation than adults', says the chairman of the American College of Radiology's Safety Committee. Later this year, he says, radiologists will expand the effort to adults. Source: http://www.usatoday.com/news/health/2010-05-05-radiation05_st_N.htm

Bar-code system lowers medication errors: study. Using a bar code on patient wristbands cut drug errors by more than half, researchers at one U.S. hospital reported on Wednesday. Researchers at Brigham and Women's Hospital in Boston found a bar-code system that matched patients with their medicines reduced the chance of getting the wrong drug by 57 percent. "Having this technology is a good thing," a doctor at Brigham and Women's said in a telephone interview. "Patients receive a lot of medications when hospitalized. It's good to have the additional safety net." The chances of getting the wrong dose fell 42 percent and of getting a drug when no doctor ordered it fell 61 percent, the doctor's team reported in the New England Journal of Medicine. Under the system, bar codes on the

patient's wristband and on the drug container let nurses cross-check the person's identity against the medicine about to be given. It is usually part of a larger electronic medication administration system that also uses bar codes. Source: http://www.reuters.com/article/idUSTRE6445NV20100505

(Kentucky) **Hard drive containing data of 5,418 patients stolen from Kentucky hospital.** A medical center in Kentucky is notifying 5,418 patients of a data breach that occurred when computer equipment, containing information on patients who underwent bone density testing, was stolen from its mammography suite. Hospital officials reported that the information on the hard drive was not encrypted, but was maintained in a locked, non-public, private area. Officials at The Medical Center at Bowling Green said the stolen piece of equipment held the data of patients who had bone density testing done between 1997 and 2009. The Medical Center at Bowling Green is a 337-bed, full service, not-for-profit hospital and is the flagship hospital for the Commonwealth Health Corporation (CHC), a not-for-profit holding company for hospital and health related businesses in South Central Kentucky and beyond. Source: http://www.healthcareitnews.com/news/hard-drive-containing-data-5418-patients-stolen-kentucky-hospital

(Pennsylvania) **Children's Tylenol recall: FDA report rips quality control at plant.** Raw materials used to make children's liquid cold medications subject to an April 30 recall were contaminated with bacteria, according to a U.S. Food and Drug Administration report released Tuesday. The recall affected 43 different Johnson & Johnson products sold under the brand names of Tylenol, Motrin, Zyrtec and Benadryl. Preliminary tests have only narrowed down the possible bacterial contaminant to a category of microorganism described as "gram negative," a broad group that includes many germs potentially harmful to humans. No injuries or illnesses have been reported in relation to the recalled products, and the FDA has said that despite finding the bacterial contaminants in the raw materials used to make the drugs, tests have yet to reveal any of the finished product to be similarly contaminated. The
report also suggested that raw material with "known contamination with gram negative organisms" were used to manufacture several finished lots of Children's and Infant's Tylenol drug products. In response to the report, the McNeil Consumer Healthcare plant in Fort Washington, Pennsylvania, where the medicines were made by the Johnson & Johnson subsidiary, has been shut down by the company indefinitely. Source: http://abcnews.go.com/GMA/OnCall/childrens-tylenol-recall-fda-report-rips-quality-control/story?id=10558014

Experts: CT scans linked to radiation overdoses. CT scans can be a lifesaving tool, but they also can cause radiation overdoses. Experts said this is happening more and more at hospitals across the country. Miscalibrated machines or operator error is exposing patients to dangerous doses of radiation. One patient went to a hospital in Huntsville, Alabama, for a routine scan. She said what happened was anything but routine. "I thought, there is something wrong with me. Then the nausea and headaches started," said the former patient. Radiation from the scan scorched part of her head and burned some of her hair off, she said. Her hair has grown back, but she still suffers from nausea, dizziness and blurry vision. "As time has gone on it has gotten worse. I keep waiting for it to get better," the former patient said. Officials are notifying about 60 patients at the same Huntsville hospital that they may have been exposed to hazardous levels of radiation. But this is not an isolated case. At Cedars Sinai Medical Center in Los Angeles, CT scans gave patients more than eight times the proper dose of radiation, officials said. In Missouri, officials said they discovered a machine used for

years was miscalibrated, exposing 76 patients to radiation overdoses. Source: http://www.wsbtv.com/2investigates/23291534/detail.html

TRANSPORTATION

(Texas) **Woman arrested after calling in false report of terrorists at airport.** A 46-year-old Midland, Texas woman was arrested early May 5 for allegedly calling 911 and falsely reporting an imminent attack on Midland International Airport by a group of terrorists. The woman was charged with false-alarm report of an emergency, a state-jail felony. Midland police said the suspect called 911 around 1:40 a.m. and "sounded intoxicated in the recording," according to an arrest affidavit. She told dispatchers certain individuals were entering the airport as terrorists. Authorities said she refused to give her full name and how she knew of the possible attack and quickly hung up. When the dispatcher tried to call back the number, she received a voicemail for the cell phone of the suspect authorities said. Dispatchers were able to use their computers to pinpoint where the call was placed. Authorities wrote that false reports are usually filed as class A misdemeanors unless the emergency involves a public primary or secondary school, public transportation, public water, gas or power supply, or other public service. Then the charge is escalated to a state-jail felony and can be punishable by six months to two years in prison and a fine not to exceed $10,000. The suspect was being held at the Midland County Detention Center on a $25,000 bond. Source: http://www.mywesttexas.com/articles/2010/05/06/news/top_stories/midland_international_airport_terrorist_mpd_fbi_creekmore.txt

(New Hampshire) **Police say 2 charged in NH bus bomb scare; 1 for resisting arrest, 1 for obstruction.** Two passengers have been arrested on May 7 in connection with a day-long bomb scare on a Greyhound bus in Portsmouth, New Hampshire. Police said a Lewiston, Maine man was charged with resisting arrest for his behavior after he got off the off the Maine-to-New York bus. Another passenger, a New York City man, was charged with obstructing officers. Both are to be arraigned in Portsmouth later May 7. The bomb scare and standoff began May 6 when a passenger reported hearing another passenger say a bomb was on the bus and called 911, prompting police to surround the bus. The overheard man was from Burundi and refused to get off the bus for many hours. He will not be charged. Source: http://www.latimes.com/news/nationworld/nation/wire/sns-ap-us-bus-bomb-threat,0,6784053.story

Bomb attempt leads to tighter No Fly List rules. The close call Monday in which a suspected terrorist nearly took off on a plane to Dubai after a botched bombing attempt in New York City has led the Transportation Security Administration to tighten procedures for checking passengers against the U.S. government's No Fly List. Effective immediately, airlines will be required to review No Fly Lists within two hours of being notified of a list update, according to an official at the U.S. Department of Homeland Security. Up to now, airlines had 24 hours to review the lists after receiving word of an update. The new requirement is designed to ensure that airlines vet "expedited additions" to the No Fly List in a timely fashion, the official said. Source: http://www.computerworld.com/s/article/9176346/Bomb_attempt_leads_to_tighter_No_Fly_List_rules_

(New York) **Security issues arise following NYC subway scare.** New York's subway system is the largest in the world, and its thousands of entrances and 800-plus miles of track make it vulnerable to

attack. On April 30, a college student disguised as a track worker exposed just how vulnerable that system is. Police said a Pace student dressed in a reflective vest, a backpack, hardhat and boots wandered for hours underground before being picked up by suspicious track workers. "In the backpack was found a can of sodium cyanide, five flares," the NYPD Commissioner said. The student told investigators he wanted to commit suicide and didn't want his body to be found, but a special team was called in to investigate the chemical being carried inside a gallon-sized paint can found in the student's possession. "Sodium cyanide does not have an explosive quality or capability but is highly toxic," the commissioner said. A security expert told CBS 2 HD, "We can go right now into any train station, walk down the platform, walk onto tracks and we're in the tunnel and it's gonna take a long time before anybody sees." The expert, a former co-chair of the New York State Anti-Terrorism Task Force, said without a completely monitored transit system, it's up to New Yorkers to be ever vigilant. "This is where the millions of riders that get on our trains every day, the workmen, everybody involved ... they see something, they report it and they take action. That's about the best we can do," he said. Police will not identify who the Pace University student is, but he has been charged with criminal trespass and is having a psychological evaluation at Bellevue Hospital. Source: http://wcbstv.com/topstories/subway.cyanide.scare.2.1666728.html

(California) **Calif. train line to unveil crash-resistant cars.** Southern California's commuter rail service is preparing to show off new crash-resistant train cars that will replace most of its older cars. The cars, which feature "crush zone" technology to absorb impact in a crash, will be unveiled Monday at Metrolink's maintenance facility in Colton. Metrolink began considering using the technology after a 2005 crash in suburban Glendale that killed 11 people. Another crash in 2008 in the San Fernando Valley killed 25 people and unleashed a second wave of concern about Metrolink safety. Metrolink hopes to have 117 cars ready by next year. The $229 million fleet is being built by Rotem, a division of Hyundai, in South Korea. Source: http://abcnews.go.com/Business/wireStory?id=10535237

Water and Dams

Beetle-infested forests pose water threat. U.S. forest managers say threats to watersheds from fire-prone dying forests are so severe they need help from local water utilities, ski resorts, and others. The crisis, experts say, is a beetle epidemic that has killed more than 17 million acres of national forest, The Denver Post reported Wednesday. The Forest Service spends nearly $1 billion a year to clear and treat beetle-ravaged forests, but it is looking for help, the newspaper said. "The federal government does not have enough resources to deal with this," said the U.S. Department of Agriculture's undersecretary for natural resources and environment. The problem is erosion and sediment, which can clog reservoirs and water delivery systems, the Post said. But enlisting the aid of local water utilities like Denver Water in funding the removal of infested trees could mean higher water rates for consumers, utility officials say. Denver Water is considering the government's request for help. "It's in our self-interest," said the president of Denver's Board of Water Commissioners. "It will be far more cost-effective to manage the watershed than it would be to wait for another forest fire to occur." Dealing with erosion after a 2002 forest fire is expected to cost Denver Water $41 million, and contractors are still dredging reservoirs and clearing pipes, the Post said. Source: http://www.upi.com/Science_News/2010/05/05/Beetle-infested-forests-pose-water-threat/UPI-29991273102365/

(Kentucky) **Kentucky River exceeds expected crest levels; homes evacuated.** The National Weather Service (NWS) in Louisville reported that the Kentucky River had already exceeded expected crest levels in Frankfort, Kentucky early Tuesday morning, and some homes were being evacuated due to flooding. At 9 a.m., the river level was already at 41.9 feet, more than 10 feet above flood level and several feet above the predicted crest of 38.4 feet, according to a NWS hydrologist. Updated projections put the crest at 42.5 feet Tuesday afternoon, he said. Flood level is around 31 feet. A spokesman for Kentucky Emergency Management said flooding has occurred in some areas and emergency officials started going door to door to conduct voluntary evacuations. He said it was crucial that residents "heed any warnings from local officials and requests for volunteer evacuations." If projections are accurate, this will be the fifth-highest crest ever recorded in Frankfort. Source: http://www.kentucky.com/2010/05/04/1251122/kentucky-river-exceeds-expected.html

EPA launches Web site listing water polluters. The Environmental Protection Agency said it's launching an interactive Web page that identifies Clean Water Act violators in communities across the country. The site has maps showing which facilities are polluting and where. The Web site is part of the EPA's Clean Water Act Action Plan aimed at helping states keep polluters in check. The page shows federal compliance information for about 40,000 permitted, smaller facilities across the country. "EPA is taking another important step to increase transparency and keep Americans informed about the safety of their local waters," said the assistant administrator for EPA's Office of Enforcement and Compliance Assurance. "Making this information more accessible and understandable empowers millions of people to press for better compliance and enforcement in their communities." Source: http://www.courthousenews.com/2010/04/30/26876.htm

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: Fusion Center (24/7): 866-885-8295(In ND only); Email: ndslic@nd.gov ; Fax: **701-328-8175**
State Radio: 800-472-2121 Bureau of Criminal Investigation: 701-328-5500 Highway Patrol: 701-328-2455
US Attorney's Office Intel Analyst: 701-297-7400 Bismarck FBI: 701-223-4875 Fargo FBI: 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, **701-328-8168**